

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SIMONA OPRIS, et al.,

Plaintiffs,

v.

SINCERA REPRODUCTIVE MEDICINE,  
formerly known as and operating as  
ABINGTON REPRODUCTIVE MEDICINE,  
P.C.,

Defendant.

CIVIL ACTION  
NO. 21-3072

**OPINION**

Slomsky, J.

May 23, 2022

**TABLE OF CONTENTS**

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>II.</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>III.</b>	<b>STANDARD OF REVIEW.....</b>	<b>3</b>
<b>IV.</b>	<b>ANALYSIS.....</b>	<b>4</b>
<b>A.</b>	<b>Count I: Negligence.....</b>	<b>4</b>
1.	Negligence .....	5
a.	Duty.....	5
b.	Breach of Duty .....	8
c.	Causation.....	8
d.	Actual Injury or Damages .....	10

2.	Negligence <u>Per Se</u> .....	14
a.	HIPAA .....	15
b.	FTC Act .....	16
<b>B.</b>	<b>Count II: Breach of Fiduciary Duty</b> .....	17
<b>C.</b>	<b>Count III: Violation of the UTPCPL</b> .....	20
<b>D.</b>	<b>Count IV: Declaratory Judgment</b> .....	24
<b>V.</b>	<b>CONCLUSION</b> .....	25

## **I. INTRODUCTION**

Cybersecurity is a topic of utmost importance in a world reliant upon technology. One particular use of technology is to store information. Despite the benefits of computerized data storage and the precautions taken to safeguard the data, maintaining sensitive personal information on a computer server leaves this data exposed to hackers and other bad actors. This case involves a class action lawsuit brought by Plaintiffs against their healthcare provider, Defendant Sincera Reproductive Medicine (“Sincera”), after a breach of their sensitive personal data. The breach occurred when a hacker accessed the healthcare facility’s computer server. Before the Court is Defendant Sincera’s Motion to Dismiss the Amended Complaint for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). (Doc. No. 17.) For reasons that follow, the Court will grant Defendant’s Motion in part and deny it in part.

## **II. BACKGROUND**

The named Plaintiffs in this case, Simona Opris, Adrian Adam, and Britney Richardson, are former patients of Defendant Sincera Reproductive Medicine (“Sincera”). (Doc. No. 15 ¶ 6.) Sincera is an entity that provides reproductive medicine to its patients. (See *id.* ¶ 17.) On May 13, 2021, Plaintiffs received a written notification from Defendant that a data breach had occurred at the healthcare center. (See *id.* ¶ 14.) The notification informed Plaintiffs that their personal identifiable information (“PII”) and protected health information (“PHI”) may have been exposed to third parties during the breach. (*Id.* ¶ 15.) This PII and PHI included, *inter alia*, patient names, driver’s license numbers, medical diagnosis and treatment information, prescription information, treating and referring physician information, and health insurance information. (*Id.* ¶ 39.)

As alleged in the Amended Complaint, on or before August 10, 2020, the data breach occurred when a hacker gained access to Sincera’s network, where all patient data was stored. (*Id.*

¶ 38.) Sincera did not contain the breach until September 13, 2020. (Id.) Because of this lapse in time, “the hacker had unlimited access to confidential patient data on [Sincera’s] networks (including Plaintiffs’ and Class Members’ breached PII and PHI) for more than one month.” (Id. ¶ 38.) Also, sometime on or before November 8, 2020, the patient information was posted on a ransomware website, Maze, on the dark web.<sup>1</sup> (Id. ¶ 40.) The Amended Complaint alleges that more than 37,000 patients of Defendant had their PII and PHI taken as a result of the breach. (Id. ¶ 43.)

On June 1, 2021, Plaintiffs initiated this case by filing a class action Complaint in the Philadelphia Court of Common Pleas. (See Doc. No. 1-1.) The Complaint identifies the class as “individuals, patients of or people that are customers of or have their records at Sincera whose PII and/or PHI was accessed and exposed to unauthorized third parties” during the data breach. (Id. ¶ 6.) On July 9, 2021, Defendant Sincera removed the case to this Court pursuant to the Class Action Fairness Act (“CAFA”), under 28 U.S.C. § 1332(d)(2). (See Doc. No. 1.)

On August 31, 2021, Plaintiffs filed an Amended Complaint. (Doc. No. 15.) The Amended Complaint alleges four claims against Defendant: (1) negligence (Count I); (2) breach of fiduciary duty and confidences (Count II); (3) violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law (“UTPCPL”), 73 P.S. § 201-1, et seq. (Count III); and (4) for a declaratory judgment under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq. (Count IV).

On September 14, 2021, Defendant Sincera filed the instant Motion to Dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. (Doc. No. 17.) In the Motion, Defendant argues that the Amended Complaint in its entirety should be dismissed. (Id. at 10.)

---

<sup>1</sup> As the Amended Complaint states, “Maze is a site where cyber attackers post data stolen from victims, including PII and PHI, in order to pressure victims to pay ransom demands.” (Doc. No. 15 ¶ 41.)

Essentially, Defendant asserts that the Amended Complaint fails to allege that Plaintiffs “are the victims of identity theft, actual or attempted,” that Plaintiffs “have made any purchases in an attempt to monitor their credit or identity,” or that Plaintiffs took particular actions “in response to the ransomware attack.” (*Id.*) Thus, Defendant seeks dismissal of Counts I, II, III, and IV.

On October 12, 2021, Plaintiffs filed a Response in Opposition to Defendant’s Motion. (Doc. No. 20.) And on October 26, 2021, Defendant filed a Reply. (Doc. No. 22.) On October 28, 2021, Defendant filed a Memorandum of Supplemental Authority, noting a recent Pennsylvania Superior Court decision, Bailey v. Hosp. of the Univ. of Pennsylvania, 266 A.3d 654 (Pa. Super. 2021).<sup>2</sup> (Doc. No. 23.) On December 21, 2021, the Court held a hearing on Defendant’s Motion to Dismiss. The matter is now fully briefed and ripe for disposition.

### III. STANDARD OF REVIEW

The motion to dismiss standard under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim is set forth in Ashcroft v. Iqbal, 556 U.S. 662 (2009). After Iqbal it is clear that “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice” to defeat a Rule 12(b)(6) motion to dismiss. *Id.* at 678; see also Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007). “To survive dismissal, ‘a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.’” Tatis v. Allied Interstate, LLC, 882 F.3d 422, 426 (3d Cir. 2018) (quoting Iqbal, 556 U.S. at 678). Facial plausibility is “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (quoting Iqbal, 556 U.S. at 678). Instead, “[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (quoting Iqbal, 556 U.S. at 678).

---

<sup>2</sup> The holding in Bailey and its application in this case is discussed infra in Section IV(A)(2)(a), “Negligence Per Se.”

Applying the principles of Iqbal and Twombly, the Third Circuit in Santiago v. Warminster Township, 629 F.3d 121 (3d Cir. 2010) set forth a three-part analysis that a district court in this Circuit must conduct in evaluating whether allegations in a complaint survive a Rule 12(b)(6) motion to dismiss:

First, the court must “tak[e] note of the elements a plaintiff must plead to state a claim.” Second, the court should identify allegations that, “because they are no more than conclusions, are not entitled to the assumption of truth.” Finally, “where there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement for relief.”

Id. at 130 (quoting Iqbal, 556 U.S. at 675, 679). The inquiry is normally broken into three parts: “(1) identifying the elements of the claim, (2) reviewing the complaint to strike conclusory allegations, and then (3) looking at the well-pleaded components of the complaint and evaluating whether all of the elements identified in part one of the inquiry are sufficiently alleged.” Malleus v. George, 641 F.3d 560, 563 (3d Cir. 2011).

A complaint must do more than allege a plaintiff’s entitlement to relief, it must “show” such an entitlement with its facts. Fowler v. UPMC Shadyside, 578 F.3d 203, 210-11 (3d Cir. 2009) (citing Phillips v. Cnty. of Allegheny, 515 F.3d 224, 234-35 (3d Cir. 2008)). “[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not ‘show[n]’—‘that the pleader is entitled to relief.’” Iqbal, 556 U.S. at 679 (second alteration in original) (citation omitted). The “plausibility” determination is a “context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” Id.

#### IV. ANALYSIS

##### A. Count I: Negligence

Count I of the Amended Complaint asserts a claim for negligence under Pennsylvania law, as well as negligence per se for failure to comply with the Federal Trade Commission Act (“FTC

Act”), 15 U.S.C. § 45(a),<sup>3</sup> and the Health Insurance Portability and Accountability Act (“HIPAA”) 42 U.S.C. § 1320(d) et seq.<sup>4</sup> In the Motion to Dismiss, Defendant asserts that the elements of a negligence claim under Pennsylvania law are not met. Additionally, Defendant argues that, under Pennsylvania law, a plaintiff may not assert negligence per se unless the statute authorizes a private right of action, “or the aim of the action is to protect a particular group of individuals.” (Doc. No. 17 at 17.) And, according to Defendant, neither is met here. In response to these arguments, Plaintiffs assert that they have pled the elements of negligence under Pennsylvania law, and there is no requirement that asserting an action for negligence per se must be authorized by statute. The Court will address each argument in turn.

### **1. Negligence**

To make out a claim of negligence under Pennsylvania law, a plaintiff must assert the following elements: (1) a duty to conform to a certain standard for the protection of others against unreasonable risks; (2) the defendant’s failure to conform to that standard, or a breach of its duty; (3) a causal connection between the conduct and the resulting injury; and (4) actual loss or damage to the plaintiff. Jones v. Plumer, 226 A.3d 1037, 1039 (Pa. Super. 2020) (quoting Brewington for Brewington v. City of Philadelphia, 199 A.3d 348, 355 (Pa. 2018)).

#### **a. Duty**

The first element of negligence is the presence of a duty. Characterizing the existence of a duty, the Amended Complaint states that, as a healthcare provider and collector of sensitive PHI and PII, “Sincera owed a duty under common law to Plaintiffs and Class Members to exercise

---

<sup>3</sup> Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” See 15 U.S.C. § 45(a)(1).

<sup>4</sup> HIPAA’s implementing regulations require that “a covered entity [] have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. 164.530(c)(2)(i).

reasonable care in obtaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.” (Doc. No. 15 ¶ 71.) Further, Plaintiffs allege that the patients were “the foreseeable and probable victims of any inadequate security practices on the part of Defendant,” and that by collecting sensitive information, “Sincera was obligated to act with reasonable care to protect against these foreseeable threats.” (*Id.* ¶ 73.) In the Motion to Dismiss, Defendant notes that “[a] duty arises only when one engages in conduct which foreseeably creates an unreasonable risk of harm to others,” concluding that the threat of a cyber-attack was not a foreseeable harm to Defendant and thus no duty arises. (Doc. No. 17 at 12–13.)

Under Pennsylvania law, those who affirmatively collect sensitive information owe a duty to exercise reasonable care to protect against the foreseeable harm of a data breach. See *Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018). In *Dittman*, the Pennsylvania Supreme Court held that an employer owed a duty to its employees to safeguard their personal information after it had collected and stored the information on its computer system. *Id.* at 1038. The *Dittman* decision was discussed in another Pennsylvania Supreme Court decision, *Feleccia v. Lackawanna Coll.*, 215 A.3d 3 (Pa. 2019). Although *Feleccia* did not involve data collection, the holding in *Dittman* decision was given in-depth analysis by the Pennsylvania Supreme Court:

In *Dittman*, for example, we recognized the legal duty of an employer (UPMC) “to exercise reasonable care to safeguard its employees’ sensitive personal information stored by the employer on an internet-accessible computer system.” *Id.* at 1038. We did so because UPMC had required its employees to provide sensitive personal information, and then collected and stored that information on its computer system without implementing adequate security measures, such as encryption, firewalls, or authentication protocols. *Id.* at 1047. We reasoned that this “affirmative conduct” by UPMC created the risk of a data breach, which in fact occurred. *Id.* We further determined that, in collecting and storing its employees’ data on its computers, UPMC owed those employees a duty to “exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act.” *Id.* *Dittman* may have been our first opportunity to recognize this duty in the context of computer systems

security, but there is longstanding jurisprudence holding that “[i]n scenarios involving an actor’s affirmative conduct, he is generally ‘under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.’” Id. at 1046, quoting Seebold, 57 A.3d at 1246. This existing duty “appropriately undergirds the vast expanse of tort claims in which a defendant’s affirmative, risk-causing conduct is in issue.” Id. at 1047, quoting Seebold, 57 A.3d at 1246, see also Dittman, 196 A.3d at 1056–57 (Saylor, CJ, concurring and dissenting) (requirement to provide confidential information as condition of employment created “special relationship” between employer and employees giving rise to duty of reasonable care to protect information against foreseeable harm).

Feleccia, 215 A.3d at 14 (2019).

The Dittman and Feleccia decisions were recently cited in In re Wawa, Inc. Data Security Litigation, No. 19-6019, 2021 WL 1818494, at \*5 (E.D. Pa. May 6, 2021) to determine if a duty existed in a data breach case. Although the claims in that case involved financial information rather than PII and PHI, the court in Wawa denied a motion to dismiss the negligence claim because, inter alia, Wawa owed a duty to protect the financial information of its customers under Dittman and Feleccia. Thus, the court held that the plaintiffs “sufficiently pled a claim for negligence based on their allegations that Wawa’s affirmative conduct, in collecting payment card information and storing it in an insecure manner, created a risk of foreseeable harm from third parties.” Wawa, Inc. Data Sec. Litig., 2021 WL 1818494, at \*7.

Here, Plaintiffs have alleged facts in the Amended Complaint showing that Sincera owed its patients a duty of care to protect their PII and PHI. Plaintiffs assert that Defendant affirmatively collected and stored sensitive PII and PHI received from Plaintiffs, which created a duty to exercise reasonable care to protect the information by implementing adequate security measures. (Doc. No. 15 ¶ 22.) Further, the Amended Complaint alleges Sincera knew that it was storing sensitive information, that any breach of its system would result in an increased risk of identity theft and fraud against patients, that PII and PHI is extremely valuable to cybercriminals, and that

cyberattacks are common for targets such as healthcare providers. (Id. ¶ 22–35.) Viewing the facts alleged as true, the Amended Complaint sufficiently establishes a duty by Defendant under Pennsylvania law to protect Plaintiffs’ PII and PHI.

**b. Breach of Duty**

To meet the second element of negligence, Plaintiff must show “[a] defendant’s failure to conform to that standard” identified in the duty analysis. See Plumer, 226 A.3d at 1039. In the Amended Complaint, Plaintiffs assert that a hacker gained access to the patients’ personal information stored on Defendant’s computer system for at least the period from August 10 to September 13, 2020, that Plaintiffs’ PII and PHI was placed on a ransomware website after the attack, and most importantly, that the data breach was a “direct result of Sincera’s failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect patients’ PII and PHI.” (Doc. No. 15 ¶ 44.) While the existence of a duty is a question of law, the issue of whether a defendant’s conduct breached that duty is typically reserved for the factfinder. Charlie v. Erie Ins. Exch., 100 A.3d 244, 260 (Pa. Super. 2014). For this reason, making a factual determination on whether Defendant violated its duty to reasonably safeguard Plaintiffs’ PII and PHI is premature at this point. But, in any case, at the motion to dismiss stage, the above allegations contain enough facts to establish a breach of duty.

**c. Causation**

Next, Defendant argues that Plaintiffs have not sufficiently pled causation, as they have not shown that the data breach was proximately caused by Defendant’s actions. (See Doc. No. 17 at 13.) “Proximate causation is defined as a wrongful act which was a substantial factor in bringing about the plaintiff’s harm.” Eckroth v. Pennsylvania Elec., Inc., 12 A.3d 422, 428 (Pa. Super. Ct. 2010). “It is not enough that a negligent act may be viewed, in retrospect, to have been one of the happenings in the series of events leading up to the injury.” Id. at 427. “A determination of legal

causation, essentially regards ‘whether the negligence, if any, was so remote that as a matter of law, [the actor] cannot be held legally responsible for [the] harm which subsequently, occurred.’” Reilly v. Tiergarten Inc., 633 A.2d 208, 209 (Pa. Super. 1993) (quoting Novak v. Jeannette Dist. Mem. Hosp., 600 A.2d 616, 618 (Pa. Super. 1991)). Ultimately, the issue of proximate causation for negligence under Pennsylvania law involves “whether the injury would have been foreseen by an ordinary person as the natural and probable outcome of the act complained of.” Id. at 209 (citing Merritt v. City of Chester, 344 Pa. Super. 505, 508, 496 A.2d 1220, 1221 (1985)).

Courts have addressed the matter of proximate cause in data breach cases and held that proximate cause is sufficiently pled when it is alleged that the defendant failed to safeguard personal information. See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 67 (D.C. Cir. 2019) (“The complaint alleges facts demonstrating proximate cause. Arnold Plaintiffs contend that OPM's failure to establish appropriate information security safeguards opened the door to the hackers, giving them ready access to a storehouse of personally identifiable and sensitive financial information.”); Stollenwerk v. Tri-West Health Care Alliance, 254 F. App'x 664, 667–68 (9th Cir. 2007) (holding, in a case where beneficiaries of a health insurance program brought a claim of negligence against the local manager of the program for failure to adequately protect personal information, that “proximate cause is supported not only by the temporal, but also by the logical, relationship” between the theft of a hard drive containing beneficiary information and the plaintiff's instance of identity theft six weeks later).

Here, Plaintiffs assert that the data breach was a “direct result of Sincera's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect patients' PII and PHI.” (Doc. No. 15 ¶ 44.) This claim is further supported by allegations that Plaintiffs provided Defendant with their PII and PHI, and that because of the breach, their

information was available and thereafter placed on a ransomware website on the dark web. (Id. ¶ 22, 40.) “Like breach of duty, causation is ordinarily a question of fact to be decided by the jury.” In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. CV 19-MD-2904, 2021 WL 5937742, at \*15 (D.N.J. Dec. 16, 2021) (citing In re Equifax, 362 F. Supp. 3d at 1319). In any event, at the motion to dismiss stage, the chain of events set forth in the Amended Complaint is sufficient to establish proximate causation.

**d. Actual Injury or Damages**

Defendant also argues that Plaintiffs have not pled facts to show an actual loss or damage occurred to demonstrate the final element of negligence. (Doc. No. 17 at 14.) Specifically, Defendant asserts that because Plaintiffs have not stated that they were the victims of “physical injury or damage to tangible property,” such as suffering from actual identity theft due to the alleged breach or securing and paying for a system to monitor their identities and personal information, their claim is insufficiently pled.<sup>5</sup> (See id. at 14–15.) To counter this assertion, Plaintiffs argue that they have suffered damages such as loss of value to their personal information, and that they have suffered mitigation damages by taking steps to reduce the risks resulting from the breach, such as purchasing credit monitoring and identity theft protection services. (Doc. No. 20 at 8–9.) Furthermore, Plaintiffs emphasize that the Amended Complaint alleges misuse of their sensitive information because the PII and PHI was posted on a ransomware site on the dark web by an unknown third party. (Doc. Nos. 15 ¶ 40, 20 at 9 n.3.)

---

<sup>5</sup> In Defendant’s Motion to Dismiss, Sincera argues that Plaintiffs have not alleged that, after the breach, they secured and paid for a system to monitor their identities and personal information. (See Doc. Nos. 17 at 15.) However, this is incorrect. The Amended Complaint states that Plaintiffs purchased credit monitoring and identity theft detection services because of the data breach. (See Doc. No. 15 ¶ 100.)

When the damages sustained by a plaintiff are foreseeable by the defendant as the “necessary, ordinary and natural consequences of its negligence,” the plaintiff is entitled to compensatory damages. See Mancine v. Concord-Liberty Sav. & Loan Ass’n, 445 A.2d 744, 747 (Pa. Super. 1982). In the Amended Complaint, under Count I, Plaintiffs state that they have suffered, inter alia, the following injuries “[a]s a direct and proximate result of Sincera’s negligence”: theft of their PII and/or PHI, the costs of credit monitoring and identity theft detection services, lowered credit scores, costs associated with time spent and the loss of productivity due to certain actions to protect against further harm, such as finding fraudulent charges and cancelling and reissuing cards, loss of value to their PII and PHI, and the increased and continued risk of exposure to hackers and thieves of their PII and PHI. (Doc. No. 15 ¶ 100.)

In arguing that these damages do not state a negligence claim, Defendant posits that the risk of future harm after a data breach, such as the increased risk of identity theft, is not a sufficient basis of recovery in a claim of negligence. (See Doc. No. 17 at 14.) To support this argument, Defendant points to several cases where courts have found that a general risk of harm did not constitute an injury-in-fact sufficient for standing, including TransUnion v. Ramirez, 141 S. Ct. 2190 (2021) (holding “mere risk of future harm,” without actual harm, does not support standing); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (holding risk of future harm insufficient for standing in data breach case where the data that was breached was never further circulated); and Browne v. US Fertility, LLC, No. 21-367, 2021 WL 2550643, at \*1 (E.D. Pa. June 22, 2021) (holding, based on Reilly, that plaintiffs did not have standing to bring claim against healthcare facility for risk of future harm after data breach).

However, in relying on these cases, Defendant has conflated the requirements of Article III standing with the requirements of negligence under Pennsylvania law. Here, Defendant does not

contend that Plaintiffs lack constitutional standing to bring this case. This stance was confirmed at the hearing held with counsel for the parties on December 21, 2021. Thus, the above cases are inapplicable here, where the issue is whether the Amended Complaint states sufficient damages to support a negligence claim, not standing.<sup>6</sup>

The allegations in the Amended Complaint satisfy the fourth element of negligence under Pennsylvania law: actual loss or injury. Although this issue has not been addressed under Pennsylvania law in data breach cases, a review of decisions from other courts reveals that mitigation damages, such as those allegedly incurred by Plaintiffs in purchasing credit and identity theft monitoring services, are a sufficient form of damages for a negligence claim. See, e.g., In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. CV 19-2904, 2021 WL 5937742, at \*16 (D.N.J. Dec. 16, 2021) (“Each of the Plaintiffs in Groups I and II adequately alleged that the hackers accessed their Personal Information, which has resulted in either tangible or intangible harm. These allegations are sufficient to satisfy the damages prong of Plaintiffs’ negligence claim at this stage.”); Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162–67 (1st Cir. 2011) (holding plaintiffs whose payment data was stolen could recover mitigation damages in negligence claim for actions taken, such as replacing credit cards and purchasing insurance “to protect against the consequences of data misuse”); Sackin v. Transperfect Glob., Inc., 278 F. Supp.

---

<sup>6</sup> Although federal courts have an “obligation to assure [them]selves of litigants’ standing under Article III,” standing has been established by Plaintiffs in this case. Unlike in Reilly, where there was a data breach and it was unknown whether the information was circulated or whether the intrusion was “intentional or malicious” (see 664 F.3d at 40, 44), Plaintiffs allege here dissemination of their information. Specifically, Plaintiffs assert that shortly after the breach, a third party posted the PII and PHI on a ransomware website on the dark web. (Doc. No. 15 ¶¶ 40–41.) Thus, the threatened harm stated here is “more ‘immanent’ and ‘impending’” than the alleged harm in Reilly. See Reilly, 664 F.3d at 44. Based on this analysis, standing is not at issue in this case because an injury-in-fact is present.

3d 739, 749 (S.D.N.Y. 2017) (“[T]he Complaint adequately alleges that Plaintiffs face an imminent threat of identity theft and have purchased preventive services to mitigate the threat. These mitigation expenses satisfy the injury requirements of negligence.”). Also, “a growing number of courts now recognize that individuals may be able to recover [c]onsequential [o]ut of [p]ocket [e]xpenses that are incurred because of a data breach, including for time spent reviewing one’s credit accounts.” In re Anthem, Inc. Data Breach Litig., No. 15-02617, 2016 WL 3029783, at \*25 (N.D. Cal. May 27, 2016) (citing Lewert v. P.F. Chang's China Bistro, Inc., No. 14-3700, 2016 WL 1459226, \*1 (7th Cir. Apr. 14, 2016)).

To find that such damages are not compensable would discourage plaintiffs from mitigating future damages that would flow from the data breach. See Sackin, 278 F. Supp. 3d at 749 (“[M]itigation expenses satisfy the injury requirements of negligence; otherwise Plaintiffs would face an untenable Catch-22 . . . Plaintiffs were required to take reasonable steps to mitigate the consequences of the data breach; they could not passively wait for their identities and money to be stolen.”).

Moreover, several courts have recognized the property value of personal information. See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 460 (D. Md. 2020) (“[T]he growing trend across courts that have considered this issue is to recognize the lost property value of this [personal] information.”) (citing In re Experian Data Breach Litig., No. SACV151592AGDFMX, 2016 WL 7973595, at \*5 (C.D. Cal. Dec. 29, 2016) (“[A] growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.”)); Calhoun v. Google LLC, No. 20-cv-05146- LHK, 2021 WL 1056532, at \*21 (N.D. Cal. Mar. 17, 2021) (recognizing property interest in personal information). Because Plaintiffs have alleged loss

of value to their PII and PHI, this assertion further supports that they suffered damages as a result of Sincera's negligence.

As Plaintiffs allege appropriate damages to support their negligence claim against Sincera, the Court will deny Defendant's Motion to Dismiss Count I of the Amended Complaint.

## **2. Negligence Per Se**

In Count I, Plaintiffs also allege negligence per se. The Amended Complaint bases its claim of negligence per se on Defendant's failure to protect Plaintiffs' personal information by alleging that this failure violated several federal statutes and a state statute. Defendant asserts in its Motion that the federal statutes underlying the negligence per se claim, Section 5 of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45(a), and the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320(d) et seq., do not provide a statutory basis for a negligence per se claim because these statutes do not create federal private rights of action. In response, Plaintiffs argue that while Defendant is correct that Section 5 of the FTC Act and HIPAA "do not create implied federal rights of private action, it does not follow that Pennsylvania common law cannot incorporate their standards in defining the sort of conduct that may give rise to negligence liability." (Doc. No. 20 at 10.)<sup>7</sup>

---

<sup>7</sup> The state statute Plaintiffs rely on to establish a duty of care for negligence per se is Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, et. seq. It provides:

The hospital shall maintain facilities and services adequate to provide medical records which are accurately documented and readily accessible to authorized persons requiring such access and which can be readily used for retrieving and compiling information.

§ 115.1. Defendants have not challenged that a duty of care arises under this statute.

“A claim of negligence per se arises out of a violation of a statute or regulation that establishes a duty.” Jordan v. City of Philadelphia, 66 F. Supp. 2d 638, 644 (E.D. Pa. 1999) (citing Taylor v. Danek Medical, Inc., 1998 WL 962062 (E.D. Pa.1998)). In essence, negligence per se uses a statutory violation to establish the first two elements of negligence, duty and breach of duty. For example, in an automobile accident case, a speed limit statute may be used as the applicable duty of care, and failure to abide by the statute would be a per se breach of this duty. See, e.g., Smith v. Wells, 212 A.3d 554, 560 (Pa. Super. 2019). Negligence per se, however, is not a separate cause of action, and is merely an alternative theory of liability. Simmons v. Simpson House, Inc., 224 F. Supp. 3d 406, 417 (E.D. Pa. 2016) (“Several courts in this Circuit have explained, however, that negligence per se is not a separate cause of action, but is instead a theory of liability that supports a negligence claim.”).

The Court has already determined that the elements of negligence under Pennsylvania law have been sufficiently pled. The Court now will determine whether the two federal statutes challenged here may be used to establish a duty of care sufficient to support a claim of negligence per se.

**a. HIPAA**

In challenging whether HIPAA creates a duty of care, Defendant has submitted a supplemental memorandum (Doc. No. 23) pointing the Court to Bailey v. Hosp. of the Univ. of Pennsylvania, 266 A.3d 654 (Pa. Super. 2021). In the memorandum, Defendant asserts that under Bailey, HIPAA may not be used as a standard of care for negligence per se in Pennsylvania. Although Bailey is a non-precedential opinion of the Pennsylvania Superior Court, it held that HIPAA may not be used by a plaintiff to establish a duty of care. In Bailey, the court stated:

Ms. Bailey avers that the court should impose a duty on healthcare providers to protect healthcare information. She further alleges that imposing the duty will

“promote the privacy goal of HIPAA.” Ms. Bailey’s [r]esponse to the [m]otion for [j]udgment on the [p]leadings notes that the [a]mended [c]omplaint’s inclusion and citation to HIPAA was done as a “standard to gage [sic] [Hospital’s] duties and the reasonableness of its action and as [an] example of how this action against [Hospital] promotes the policy goals of HIPAA and 28 Pa. Code § 115.27.” Ms. Bailey’s [Rule] 1925(b) [s]tatement similarly states that she only “mentions” HIPAA “to enunciate the standard of care and policy goals these laws already apply to [Hospital].” Because HIPAA does not confer a private right of action, HIPAA cannot be the source of the duty supposedly owed to Ms. Bailey.

\* \* \*

Given Ms. Bailey’s undeveloped arguments below concerning any common law duty, we agree with the trial court that Hospital is entitled to judgment as a matter of law on this issue. Ms. Bailey did not demonstrate that a common law duty exists, or should exist, to support her negligence cause of action. As a result, based on the arguments before it, the trial court reasonably concluded that Ms. Bailey fails to identify any other source of a duty of care [besides HIPAA and 28 Pa. Code. § 115.27] that . . . [the] Hospital owed to her. In the absence of an actionable duty, there can be no negligence claim.

Id. at \*6. Even though the words “negligence per se” are not used in Bailey, its holding is on point and supports Defendant’s position that HIPAA and its implementing regulations cannot be relied upon to establish a duty of care for a negligence per se claim in Pennsylvania. Therefore, the Court will dismiss the Amended Complaint’s negligence per se claim based upon HIPAA.

#### **b. FTC Act**

No court decision has been brought to the attention of the Court that held that Section 5 of the FTC Act does not create a duty of care in a negligence per se claim. In In re Rutter’s Inc. Data Security Breach Litigation, and in Wawa, discussed supra, the district courts were confronted with the same challenge as to whether Section 5 of the FTC Act established a duty of care. However, both courts decided that the best stage at which to make a decision on this issue was either at the summary judgment stage or during pre-trial motion practice. See In re Rutter’s Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 532 (M.D. Pa. 2021) (“Summary judgment or pre-trial motion practice are more appropriate vehicles to analyze the applicability of the FTC Act as a predicate

for a Pennsylvania negligence *per se* claim than the motion.”). In Wawa, the court adopted Rutter’s approach:

Wawa argues that the [plaintiffs’] negligence *per se* claim must be dismissed because the FTC Act does not provide a private right of action. Wawa contends that under Pennsylvania law, “if a statute does not provide for a private cause of action, a negligence *per se* claim based on that statute will not lie.” But the Court agrees with the approach taken by the court in Rutter’s. There, after dismissing the plaintiffs’ negligence *per se* claim while finding that their negligence claim could proceed, that court declined to “reach a decision on the viability” of an alternative theory of negligence at the motion to dismiss stage. Rutter’s, 2021 WL 29054, at \*11. Instead, it noted that a motion for summary judgment or pre-trial motion practice would be a more appropriate vehicle “to analyze the applicability of the FTC Act as a predicate for a Pennsylvania negligence *per se* claim.” *Id.*<sup>8</sup>

In re Wawa, Inc. Data Sec. Litig., No. 19-6019, 2021 WL 1818494, at \*7 (E.D. Pa. May 6, 2021).

The Court will adopt this approach here, and at this stage, Defendant’s Motion to Dismiss the part of Count I that uses Section 5 of the FTC Act as a standard of care for negligence *per se* will be denied. The Court, however, will consider this argument at the summary judgment stage.

As noted above, because Plaintiffs have stated facts to support a common law negligence claim, Count I will remain, except for the negligence *per se* claim asserted under HIPAA, which will be dismissed.

## **B. Count II: Breach of Fiduciary Duty**

In Count II, Plaintiffs claim that Defendant’s conduct constituted a breach of its fiduciary duty to Plaintiffs.<sup>9</sup> (Doc. No. 15 ¶ 112.) To establish breach of a fiduciary duty in Pennsylvania,

---

<sup>8</sup> In Rutter’s, the court dismissed the negligence *per se* claim relying upon a duty of care under the FTC Act because it was improperly pled in a separate count from the negligence claim. The court dismissed the claim without prejudice “if [the plaintiffs] wish[ed] to employ a negligence *per se* theory to satisfy the duty and breach elements of Count I at a later time.” 511 F. Supp. 3d at 533. Here, the negligence claim and the negligence *per se* claim are both included in Count I.

<sup>9</sup> In Count II, Plaintiffs also assert that Defendant has breached its “duty of confidences.” From the face of the Amended Complaint, it is unclear whether Plaintiffs intended to assert “breach

the claimant must show: “(1) that the defendant negligently or intentionally failed to act in good faith and solely for the benefit of plaintiff in all matters for which he or she was employed; (2) that the plaintiff suffered injury; and (3) that the agent’s failure to act solely for the plaintiff’s benefit . . . [was] a real factor in bring[ing] about plaintiff’s injuries.” Dinger v. Allfirst Fin., Inc., 82 F. App’x 261, 265 (3d Cir. 2003) (quoting McDermott v. Party City Corp., 11 F.Supp.2d 612, 626 n.18 (E.D. Pa.1998)).

Pennsylvania courts have recognized a fiduciary duty where there exists a “confidential relationship,” which appears when the parties “do not deal on equal terms, but, on the one side there is an overmastering influence, or, on the other, weakness, dependence or trust, justifiably reposed.” Vicky M. v. Ne. Educ. Intermediate Unit 19, 486 F. Supp. 2d 437, 458 (M.D. Pa. 2007), on reconsideration, No. 06-01898, 2007 WL 2844428 (M.D. Pa. Sept. 26, 2007) (citing Leedom v. Palmer, 117 A. 410, 411 (Pa. 1922)). Further, a confidential relationship exists “as a matter of fact whenever one person has reposed a special confidence in another to the extent that the parties do not deal with each other on equal terms, either because of an overmastering dominance on one side, or weakness, dependence or justifiable trust, on the other.” In re Clark’s Est., 359 A.2d 777, 781 (Pa. 1976) (quotation marks, ellipses, and citations omitted).

More specifically for purposes of this case, courts have previously characterized the doctor-patient relationship as one where a fiduciary relationship exists under Pennsylvania law. Doe v.

---

of the duty of confidences” as a separate claim, as it is included in the heading and language of Count II along with the claim for breach of fiduciary duty. As the Court will discuss, a confidential relationship may serve as the basis for a fiduciary relationship. In any event, Plaintiffs are required to set forth each cause of action in a separate Count. FED. R. CIV. P. 10(b). Thus, for purposes of Defendant’s Motion to Dismiss, the Court need not discuss the viability of a separate claim for “breach of confidence” because Count II will survive Defendant’s Motion as stating a claim for breach of fiduciary duty.

Liberatore, 478 F. Supp. 2d 742, 767 (M.D. Pa. 2007) (noting the “higher level associations involved in fiduciary relationships such as attorney and client, doctor and patient, or clergy and penitent”) (citations omitted); Moses v. McWilliams, 549 A.2d 950, 964 (Pa. Super. 1988) (Cirillo, J., concurring in part) (“Society is concerned not merely with the health of the community, but with the dignity and privacy of its members. That dignity and privacy are violated where the fiduciary relationship between a patient and physician—a relationship built on the highest expectation of trust—is betrayed.”); Alexander v. Knight, 177 A.2d 142, 146 (Pa. Super. 1962) (“We are of the opinion that [members] of a profession, especially the medical profession, stand in a confidential or fiduciary capacity as to their patients. They owe their patients more than just medical care for which payment is exacted; there is a duty of total care . . . .”).

Here, construing the facts in the Amended Complaint as true, Plaintiffs have established that a fiduciary relationship existed between Plaintiffs, who were patients, and Defendant, their medical provider, under Pennsylvania law. Also, Plaintiffs have pled sufficient facts to show, at this stage, that Sincera breached its fiduciary duty to safeguard their sensitive personal and medical information, or their PII and PHI, and that this conduct caused their injuries. In the Amended Complaint, Plaintiffs argue that “as a healthcare provider, Sincera has a fiduciary relationship to its patients,” and that “[b]ecause of that fiduciary and special relationship, Sincera was provided with and stored private and valuable PHI related to Plaintiffs and the Class, which it was required to maintain in confidence.”<sup>10</sup> (Doc. No. 15 ¶¶ 103–04.) Also, the Amended Complaint states that such records contained information concerning “personal medical matters” and that Plaintiffs did not consent to the release of this information. (Id. ¶¶ 108–10.) To demonstrate breach, Plaintiffs

---

<sup>10</sup> Additionally, as noted in Plaintiffs’ Response, “Sincera is a fertility provider,” and “[u]ndergoing fertility treatment, or even considering doing so, is a profoundly personal matter that no one could want to be indiscriminately disclosed to the public.” (Doc. No. 20 at 11 n.4.)

assert, inter alia, that Sincera “mismanage[ed] its system,” that Sincera “mishandle[ed] its data security by failing to assess the sufficiency of its safeguards in place to control these risks,” that Sincera “fail[ed] to detect the breach at the time it began or within a reasonable time thereafter.” (Id. ¶ 111.) Finally, Plaintiffs state that they suffered injuries, as discussed above, including theft of their PII and PHI, costs associated with credit monitoring and preventing identity theft, lowered credit scores, and erosion of the confidential relationship between Plaintiffs and Sincera, and that “but for Sincera’s wrongful breach . . . their privacy, confidences, PII and PHI would not have been compromised.” (Id. ¶ 113–14.)

In the above allegations, Plaintiffs have sufficiently alleged a confidential, patient-doctor relationship between themselves and Defendant sufficient to satisfy the definition of a fiduciary relationship under Pennsylvania law. The Complaint alleges not only that Sincera was the fiduciary of Plaintiffs’ personal identifying information (“PII”), but also was given, in confidence, their protected health information (“PHI”) relating to their treatment at Sincera and other health facilities. Also, the above allegations state that Sincera “negligently or intentionally failed to act in good faith,” that Plaintiffs suffered injuries, and that Sincera caused such injuries through its failure to safeguard information and adequately respond to the breach. See Dinger, 82 F. App’x at 265. These facts sufficiently allege injuries and causation. Therefore, Count II of the Amended Complaint will survive Defendant’s Motion to Dismiss because it sufficiently states a claim for breach of fiduciary duty.

### **C. Count III: Violation of the UTPCPL**

In Count III, Plaintiffs allege a violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law (“UTPCPL”), 73 P.S. § 201-1, et seq. The UTPCPL provides:

Any person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money

or property, real or personal, as a result of the use or employment by any person of a method, act or practice declared unlawful by section 3 of this act, may bring a private action to recover actual damages or one hundred dollars (\$100), whichever is greater.

73 P.S. § 201-9.2(a). To establish liability under the UTPCPL, a party must prove: “(1) a deceptive act that is likely to deceive a consumer acting reasonably under similar circumstances; (2) justifiable reliance; and (3) that the plaintiff’s justifiable reliance caused ascertainable loss.”

Slapikas v. First Am. Title Ins. Co., 298 F.R.D. 285, 292 (W.D. Pa. 2014).

In the instant Motion and Reply, Defendant only discusses the third element, “ascertainable loss,” and argues that Count III should be dismissed because this requirement of the UTPCPL is not met. (Doc. No. 17 at 21.) In support of this assertion, Defendant opines that voluntary actions, “such as time allegedly spent monitoring credit,” do not qualify as an actionable “ascertainable loss.” (*Id.* at 21.) In their Response, Plaintiffs assert that, regarding the first and second elements, because Sincera received payment for its services as a healthcare provider “with the understanding that Sincera would maintain the privacy of their information, which it then failed to do,” this misrepresentation constituted Sincera engaging in fraudulent or deceptive conduct.<sup>11</sup> (Doc. No. 20 at 15.)

---

<sup>11</sup> Although Defendant has not argued in its filings that the first and second elements are not met, the Court nevertheless notes that the allegations in the Amended Complaint are sufficient to establish these elements at this juncture. The Amended Complaint lists a number of “unfair or deceptive acts and practices,” including “[m]isrepresenting that it would protect the privacy and confidentiality of Plaintiffs’ and Class members’ PII and PHI, including by implementing and maintaining reasonable security measures,” “[m]isrepresenting that certain sensitive PII and PHI was not accessed during the Data Breach, when it was,” and “[o]mitting, suppressing, and concealing the material fact that it did not reasonably and adequately secure Plaintiffs’ and Class members’ PII and PHI.” (Doc. No. 15 ¶¶ 121–22.) Further, the Amended Complaint asserts that these acts “induce[d] [Plaintiffs] to rely on its misrepresentations” and caused Plaintiffs to believe “that their PII and PHI was secure and that they did not need to take actions to secure their identities” when giving their information to Sincera for healthcare services, as well as during the month-long data breach when they allege that Sincera failed to notify them or contain the breach. (*Id.* ¶¶ 124.)

To show that a defendant's actions caused "ascertainable loss" under the UTPCPL, "[a]n actual loss of money or property must have occurred to state a cognizable UTPCPL claim." Allen v. Wells Fargo, N.A., No. CV 14-5283, 2015 WL 5137953, at \*8 (E.D. Pa. Aug. 28, 2015). These damages must be identifiable and "cannot be speculative." Jarzyna v. Home Properties, L.P., 185 F. Supp. 3d 612, 626 (E.D. Pa. 2016), *aff'd*, 783 F. App'x 223 (3d Cir. 2019). In the data breach context, costs associated with the breach must constitute an "ascertainable loss," and mere allegations that the plaintiff just spent time "dealing with" the breach, without alleging costs, is not sufficient. In re Rutter's Inc. Data Security Breach Litigation, 511 F. Supp. 3d 514, 541 (M.D. Pa. 2021). ("While Plaintiff Collins dedicated approximately five hours "dealing with" the breach through various "remedial actions," there is no allegation that he lost any money as a result.")

Here, the allegations in the Amended Complaint are distinguishable from those of the plaintiffs in Rutter's. In the Amended Complaint, Plaintiffs have alleged costs associated with the data breach, such as purchasing credit monitoring and identity theft detection services. (Id. ¶ 100.) Such costs constitute "ascertainable loss" of money or property under the UTPCPL that surpass lost time. Also, Plaintiffs have asserted that they purchased these services because of the Sincera data breach, thus alleging an "ascertainable loss" that was caused by the alleged acts of Defendant to sufficiently plead the third element of a claim under the UTPCPL. (See id. ¶ 128.) Further, as discussed supra, Plaintiffs have alleged lost property value to their PII and PHI, which serves as another form of lost property.

---

These allegations, if true, suffice at the motion to dismiss stage to establish deceptive acts by Sincera and justifiable reliance by Plaintiffs.

Regarding whether voluntary actions can satisfy the “ascertainable loss” requirement, Defendant’s reliance on Grimes v. Enterprise Leasing Company of Philadelphia, LLC, 105 A.3d 1188 (Pa. 2014) is misplaced. While Grimes held that attorney fees are not “ascertainable losses” under the UTCPL, the court came to this conclusion not necessarily because the plaintiff’s decision to hire counsel was “voluntary,” but because the UTCPL “initially provides for damages relative to ‘ascertainable loss[es],’ then separately provides for awards of ‘costs and reasonable attorney fees.’” Id. at 1194 (citing 73 P.S. § 201–9.2(a)). Although the court agreed that categorizing attorney fees under the third element “would allow a plaintiff to manufacture” an ascertainable loss in every instance they have hired counsel to litigate a claim under the UTCPL, this conclusion arose from an analysis of separate treatment of both attorney’s fees and costs under the statute, rather than solely because hiring counsel was “voluntary.” Id. at 1193. Here, Plaintiffs’ asserted costs are in purchasing monitoring services and lost value to their PII and PHI, prior to hiring an attorney to litigate the instant lawsuit. These are not attorney’s fees, and therefore Grimes is not determinative.

Discovery in this case will reveal whether Plaintiffs secured and paid for identity theft protection and credit monitoring and whether Plaintiffs’ PII and PHI lost value because of the alleged data breach. Nevertheless, at this stage, the Court must assume these facts as true and will deny Defendant’s Motion to Dismiss Count III of the Amended Complaint because Plaintiffs have alleged an “ascertainable loss.”

#### **D. Count IV: Declaratory Judgment**

Last, Plaintiffs assert a claim to relief under the federal Declaratory Judgment Act.<sup>12</sup> The DJA provides that “[i]n a case of actual controversy within its jurisdiction . . . any court of the United States . . . may declare the rights and other legal relations of any interested party seeking such declaration, whether further relief is or could be sought.” 28 U.S.C. § 2201(a). The Third Circuit has set forth the following factors to consider when entertaining a claim under the Declaratory Judgment Act: “(1) the likelihood that the declaration will resolve the uncertainty of obligation which gave rise to the controversy; (2) the convenience of the parties; (3) the public interest in a settlement of the uncertainty of obligation; and (4) the availability and relative convenience of other remedies.” Founders Ins. Co. v. Bustleton Spirits, Inc., No. 12-1303, 2012 WL 13015113, at \*2 (E.D. Pa. June 26, 2012) (citing Terra Nova Ins. Co. v. 900 Bar. Inc., 887 F.2d 1213, 1224 (3d Cir. 1989)) (internal quotation marks omitted).

“Where there is ‘some overlap’ between plaintiffs’ declaratory judgment claim and other substantive claims, courts may refuse to dismiss the declaratory judgment claim if the plaintiffs’ ‘remaining claims have not been fully developed . . . [and] the Court cannot fully evaluate the extent of the overlap to determine whether declaratory judgment would serve [any] useful purpose

---

<sup>12</sup> In Defendant’s Motion to Dismiss, Plaintiffs’ Response, and Defendant’s Reply, the parties discuss the viability of Count IV under the Pennsylvania Declaratory Judgment Act, 42 P.S. § 7532. (See Doc. No. 17 at 22, Doc. No. 20 at 17, Doc. No. 22 at 10.) However, in the Amended Complaint, Plaintiffs assert Count IV under the federal Declaratory Judgment Act (“DJA”), 28 U.S.C. §§ 2201, et seq.

In any event, in a removed declaratory judgment action, such as this case, the federal Declaratory Judgment Act (“DJA”) governs, and not the state declaratory judgment act. Gibbons v. Mid-Century Ins. Co., 489 F. Supp. 3d 325, 329 n.2 (E.D. Pa. 2020) (“Although Plaintiffs requested relief under the Pennsylvania Declaratory Judgments Act, 42 Pa.C.S. § 7531, in the removed declaratory judgment action, the DJA, and not the state declaratory judgment law, governs.”).

in clarifying the legal rights and relationships at issue.” Baker v. Deutschland GmbH, 240 F. Supp. 3d 341, 350 (M.D. Pa. 2016) (citing Fleisher v. Fiber Composites, LLC, 2012 WL 5381381, at \*12–13 (E.D. Pa. Nov. 2, 2012)).

Here, Plaintiffs seek a declaration that “Sincera owes a legal duty to secure PII and PHI and to timely notify patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law,” as well as that “Sincera continues to breach this legal duty by failing to employ reasonable measures to secure consumers’ PII and PHI.” (Doc. No. 15 ¶ 133.) The sought declaration overlaps with the rest of Plaintiffs’ Amended Complaint. Whether the Court should issue such a declaration will depend on the outcome of Plaintiff’s substantive claims in Counts I, II, and III. At the motion to dismiss stage, these claims have not been fully developed. Thus, dismissal of Plaintiffs’ claim under the DJA would be premature. If Plaintiffs develop their claims in Counts I, II, and III, the Court will then look to the factors outlined by the Third Circuit to determine whether a declaratory judgment is an appropriate remedy. For these reasons, the Court will not dismiss Plaintiff’s declaratory judgment claim under the Federal Declaratory Judgment Act.

## **V. CONCLUSION**

For the foregoing reasons, the Court will grant in part and deny in part Defendant’s Motion to Dismiss (Doc. No. 17.) An appropriate Order follows.